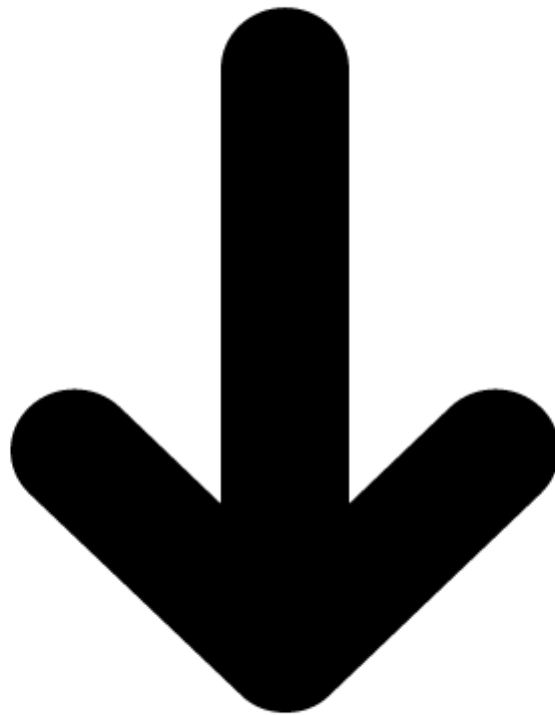


## **Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata**

Nama Kelompok :

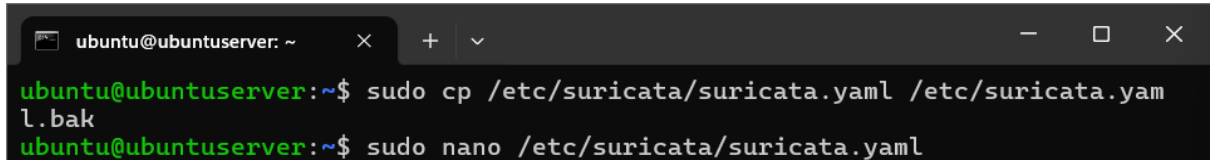
- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah



## Konfigurasi interface & basic rules Suricata

### \*Konfigurasi

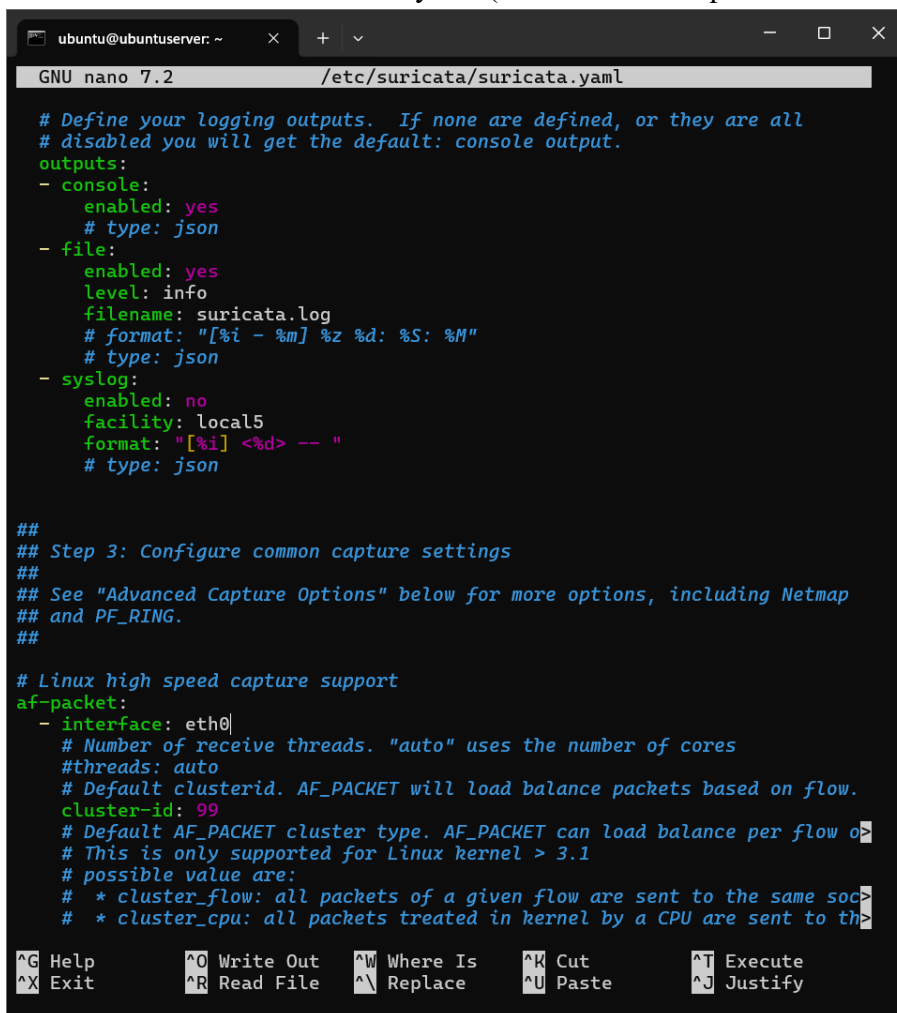
1. `sudo cp /etc/suricata/suricata.yaml /etc/suricata.yaml.bak`



```
ubuntu@ubuntu-server: ~  
ubuntu@ubuntu-server:~$ sudo cp /etc/suricata/suricata.yaml /etc/suricata.yaml.bak  
ubuntu@ubuntu-server:~$ sudo nano /etc/suricata/suricata.yaml
```

Melakukan backup file konfigurasi default Suricata ( Langkah ini dilakukan untuk memastikan bahwa konfigurasi asli tetap aman apabila suatu saat diperlukan pemulihan. )

2. `sudo nano /etc/suricata/suricata.yaml` ( Edit section `af-packet interface:enp0s8` )



```
GNU nano 7.2 /etc/suricata/suricata.yaml  
  
# Define your logging outputs. If none are defined, or they are all  
# disabled you will get the default: console output.  
outputs:  
- console:  
  enabled: yes  
  # type: json  
- file:  
  enabled: yes  
  level: info  
  filename: suricata.log  
  # format: "[%i - %m] %z %d: %S: %M"  
  # type: json  
- syslog:  
  enabled: no  
  facility: local5  
  format: "[%i] <%d> -- "  
  # type: json  
  
##  
## Step 3: Configure common capture settings  
##  
## See "Advanced Capture Options" below for more options, including Netmap  
## and PF_RING.  
##  
# Linux high speed capture support  
af-packet:  
- interface: eth0|  
  # Number of receive threads. "auto" uses the number of cores  
  #threads: auto  
  # Default clusterid. AF_PACKET will load balance packets based on flow.  
  cluster-id: 99  
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow o  
  # This is only supported for Linux kernel > 3.1  
  # possible value are:  
  # * cluster_flow: all packets of a given flow are sent to the same soc  
  # * cluster_cpu: all packets treated in kernel by a CPU are sent to th
```

Melakukan pengeditan file `suricata.yaml` untuk menyesuaikan interface jaringan yang akan dipantau. ( Pada bagian `af-packet`, interface diubah menjadi `enp0s8` agar Suricata menangkap lalu lintas pada interface tersebut. )

3. `sudo mkdir -p /var/log/suricata`
4. `sudo chmod 755 /var/log/suricata`
5. `sudo chown suricata:suricata /var/log/suricata`

```
ubuntu@ubuntu-server: ~$ sudo cp /etc/suricata/suricata.yaml /etc/suricata.yaml.bak
ubuntu@ubuntu-server: ~$ sudo nano /etc/suricata/suricata.yaml
ubuntu@ubuntu-server: ~$ sudo nano /etc/suricata/suricata.yaml
ubuntu@ubuntu-server: ~$ sudo nano /etc/suricata/suricata.yaml
ubuntu@ubuntu-server: ~$ sudo mkdir -p /var/log/suricata
ubuntu@ubuntu-server: ~$ sudo chmod 755 /var/log/suricata
ubuntu@ubuntu-server: ~$ sudo chown suricata:suricata /var/log/suricata
```

- Membuat direktori log Suricata ( `sudo mkdir -p /var/log/suricata` ) Direktori ini digunakan sebagai lokasi penyimpanan seluruh output log dari Suricata.
- Mengatur permissions direktori log ( `sudo chmod 755 /var/log/suricata` `sudo chown suricata:suricata /var/log/suricata` ) Langkah ini memastikan Suricata memiliki hak akses penuh untuk menulis log ke direktori tersebut.

6. `sudo suricata -T -c /etc/suricata/suricata.yaml -I enp0s8` (test configuration)

```
ubuntu@ubuntu-server: ~$ sudo suricata -T -c /etc/suricata/suricata.yaml -i enp0s8
i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
i: mpm-hs: Rule group caching - loaded: 113 newly cached: 0 total cacheable: 113
i: suricata: Configuration provided was successfully loaded. Exiting.
i: device: enp0s8: packets: 0, drops: 0 (0.00%), invalid checksum: 0
ubuntu@ubuntu-server: ~$
```

Melakukan pengujian konfigurasi ( Perintah ini berfungsi untuk memeriksa apakah file konfigurasi sudah benar. Jika muncul pesan “*Configuration provided was successfully loaded*”, maka konfigurasi berhasil dan tidak terdapat error. )

## \*basic rules Suricata

### \*Rule

1. `alert tcp any any -> $HOME_NET any (msg:"[SURICATA] Port Scan Terdeteksi"; flags:S; threshold:type threshold, track by_src, count 5, seconds 3; sid:1000001; rev:1;)`

( Rule ini akan memicu alert apabila terdapat 5 koneksi SYN dalam waktu 3 detik dari satu sumber yang sama, yang biasanya mengindikasikan aktivitas port scanning. )

2. `alert tcp any any -> $HOME_NET 22 (msg:"[ALERT] Banyak Koneksi ke SSH - Kemungkinan brute-force"; flags:S; threshold:type both, track by_src, count 5, seconds 60; sid:1000004; rev:1;)`

( Rule ini mendeteksi adanya banyak koneksi menuju port SSH (22) dalam waktu singkat, yang merupakan ciri serangan brute-force login. )

1. `sudo cp -r /etc/suricata/rules /etc/suricata/rules.backup`

```
ubuntu@ubuntu-server: ~$ sudo cp -r /etc/suricata/rules /etc/suricata/rules.backup
[sudo] password for ubuntu:
ubuntu@ubuntu-server: ~$
```

( Membuat backup folder rules )

## 2. sudo suricata-update

```
ubuntu@ubuntu-server: ~  
[sudo] password for ubuntu:  
ubuntu@ubuntu-server:~$ sudo suricata-update  
[sudo] password for ubuntu:  
20/11/2025 -- 10:42:43 - <Info> -- Using data-directory /var/lib/suricata.  
20/11/2025 -- 10:42:43 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml  
20/11/2025 -- 10:42:43 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.  
20/11/2025 -- 10:42:43 - <Info> -- Found Suricata version 8.0.2 at /usr/bin/suricata.  
20/11/2025 -- 10:42:43 - <Info> -- Loading /etc/suricata/suricata.yaml  
20/11/2025 -- 10:42:43 - <Info> -- Disabling rules for protocol pgsql  
20/11/2025 -- 10:42:43 - <Info> -- Disabling rules for protocol modbus  
20/11/2025 -- 10:42:43 - <Info> -- Disabling rules for protocol dnp3  
20/11/2025 -- 10:42:43 - <Info> -- Disabling rules for protocol enip  
20/11/2025 -- 10:42:43 - <Info> -- No sources configured, will use Emerging Threats Open  
20/11/2025 -- 10:42:43 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-8.0.2/emerging.rules.tar.gz.md5.  
20/11/2025 -- 10:42:44 - <Info> -- Remote checksum has not changed. Not fetching.  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dhcp-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dnp3-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dns-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/files.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http2-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ipsec-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/kerberos-events.rules  
20/11/2025 -- 10:42:45 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/modbus-events.rules
```

**Mengupdate rules Suricata** ( Tahapan ini digunakan untuk memperbarui rule-rule dari komunitas (ET Open Rules). )

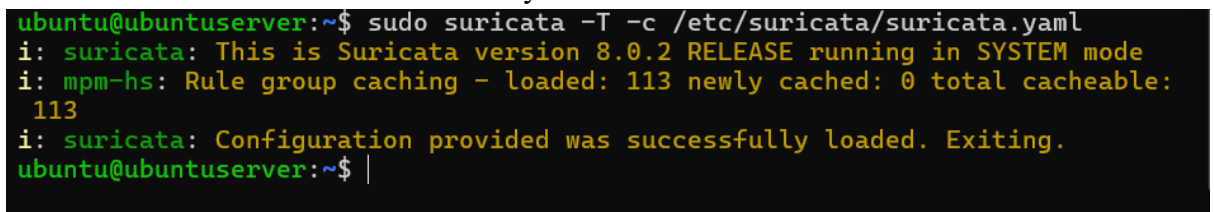
3. `sudo nano /etc/suricata/rules/local.rules`



```
ubuntu@ubuntu-server: ~  
GNU nano 7.2 /etc/suricata/rules/local.rules *  
alert tcp any any -> $HOME_NET any (msg:"[SURICATA] Port Scan Terdeteksi"; >  
alert tcp any any -> $HOME_NET 22 (msg:"[ALERT] Banyak Koneksi ke SSH - Kem>  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify
```

**Menambahkan rule local** ( Pada file inilah kedua rule yang telah dibuat sebelumnya disimpan.)

4. `sudo suricata -T -c /etc/suricata/suricata.yaml`



```
ubuntu@ubuntu-server:~$ sudo suricata -T -c /etc/suricata/suricata.yaml  
i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode  
i: mpm-hs: Rule group caching - loaded: 113 newly cached: 0 total cacheable:  
113  
i: suricata: Configuration provided was successfully loaded. Exiting.  
ubuntu@ubuntu-server:~$ |
```

**Melakukan pengujian konfigurasi Kembali** ( Pengujian ini memastikan rule lokal dan konfigurasi Suricata sudah benar dan siap digunakan. )

